Light is OSRAM

OSRAM BCR

Bindende Unternehmensrichtlinie (Binding Corporate Rules - „BCR“) für OSRAM-Konzerngesellschaften und beitretende Gesellschaften zum Schutz personenbezogener Daten

Definitionen

- **Beitretende Gesellschaft** eine in- oder ausländische OSRAM-Beteiligungsgesellschaft, an der die OSRAM Konzernobergesellschaft oder ein verbundenes Unternehmen eine Minderheitsbeteiligung hält und die sich mit Zustimmung der OSRAM Konzernobergesellschaft auf freiwilliger Basis durch die Unterzeichnung eines ICA auf die Regelungen der BCR verpflichtet hat;
- **BCR** die vorliegenden Binding Corporate Rules und die darin enthaltenen Regelungen;

- **Einwilligung** eine ohne Zwang, spezifische, informierte und unzweideutige Willensäußerung, bei der die betroffene Person durch eine Erklärung oder eine klare positive Handlung ihr Einverständnis mit der Verarbeitung sie betreffender personenbezogener Daten bekundet[1];

- **Verantwortlicher** die Stelle (natürliche oder juristische Person, Behörde oder sonstige rechtlich selbständige Stelle), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet;

- **CDPD** Corporate Data Privacy Department, die gemäß OSRAM Organisationsplan für den konzernweiten Datenschutz zuständige zentrale Abteilung des OSRAM Konzerns;

- **Kunden und Lieferanten** die natürlichen und juristischen Personen, mit denen eine Geschäftsbeziehung besteht oder geplant ist;

- **Betroffener / Betroffene Person** jede bestimmte oder bestimmbare natürliche Person, deren Daten verarbeitet werden. Bestimmbar ist eine Person dann, wenn sie direkt oder indirekt identifiziert werden kann, z. B. durch Bezugnahme auf einen spezifischen Identifikator oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind; Juristische Personen können durch entsprechende Vereinbarung zwischen der datenübermittelnden Gesellschaft und dem Datenempfänger in den Geltungsbereich der BCR einbezogen werden und gelten insoweit als Betroffene;

- **DPC** den Data Protection Coordinator, d.h. Datenschutzkoordinator die von einem teilnehmenden Unternehmen benannte Person, die für die lokale Umsetzung und Einhaltung der BCR sowie für die Unterstützung der CDPD verantwortlich ist;

- **DPE** den Data Protection Executive einer Konzerngesellschaft; diese Position wird vom jeweiligen CEO der Konzerngesellschaft wahrgenommen;

- **DPO** Data Protection Officer, d.h. die von einem teilnehmenden Unternehmen ernannte Person, die die Geschäftsleitung in Fragen der lokalen Umsetzung und Einhaltung der Allgemeinen Datenschutzverordnung und anderer anwendbarer Datenschutzbestimmungen beaufsichtigt und berät und deren Ernennung unter bestimmten, darin festgelegten Bedingungen obligatorisch ist;
- **EWR-Land / EWR-Länder** die Mitgliedsstaaten der Europäischen Union (EU) sowie die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR);

[1] Bestimmte nationale Gesetzgebungen können besondere Anforderungen an die Einwilligung stellen, was die Gültigkeit der Einwilligung beeinträchtigen kann.

- **Datenschutz-Grundverordnung (DSGVO)** die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

- **Konzerngesellschaft bzw. OSRAM-Konzerngesellschaft** die OSRAM Konzernobergesellschaft und jede in- oder ausländische Gesellschaft, an denen die OSRAM Konzernobergesellschaft direkt oder indirekt mit Mehrheit beteiligt ist bzw. die Mehrheit der Stimmrechte oder die Managementkontrolle besitzt;

- **ICA** Inter-Company Agreement, durch dessen Beitritt sich ein Unternehmen des OSRAM-Konzerns zur Einhaltung der Bestimmungen der BCR verpflichtet;

- **OSRAM Konzernobergesellschaft** die OSRAM GmbH;

- **Teilnehmende Gesellschaft** eine OSRAM-Konzerngesellschaft oder eine beitretende Gesellschaft, die dem ICA beitritt und sich damit zur Einhaltung der Bestimmungen dieser BCR verpflichtet;

- **Personenbezogene Daten** alle Informationen über einen Betroffenen;

- **Verletzung personenbezogener Daten** eine Sicherheitsverletzung, die zur unbeabsichtigten oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt;

- **Verarbeitung personenbezogener Daten** oder **Datenverarbeitung** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten - wie etwa das Erheben, Speichern, die Organisation, Strukturierung, Aufbewahrung, die Anpassung oder Veränderung, das Abfragen, die Konsultation, Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder sonstige Bereitstellung, die Angleichung oder Kombination sowie die Löschung, die Vernichtung oder die Einschränkung der Verarbeitung;

- **Auftragsverarbeiter** die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet;

- Besondere **Kategorien personenbezogener Daten** Informationen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; genetische Daten und biometrische Daten, die zur eindeutigen Identifizierung einer natürlichen Person verwendet werden, Daten über die Gesundheit oder Daten über das Sexualleben oder die sexuelle Ausrichtung eines natürlichen Individuums;

- **Standard-Vertragsklauseln** EU-Standardvertragsklauseln für Datenverarbeiter, die durch den Beschluss der Europäischen Kommission 2010/87/EU angenommen wurden, oder EU-Standardvertragsklauseln zwischen Datenverarbeitern, die durch den Beschluss 2011/497/EG oder 2004/915/EG angenommen wurden, oder andere vertragliche Garantien, die durch Beschlüsse der Europäischen Kommission gemäß Artikel 46 Absatz 2 (c) der Datenschutz-Grundverordnung angenommen wurden;

- **Dritter** jede natürliche oder juristische Person, Behörde, Einrichtung oder Stelle außer der betroffenen Person, des Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der direkten Aufsicht des Verantwortlichen oder des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten;

- **Beitretende Gesellschaft** eine in- oder ausländische OSRAM-Beteiligungsgesellschaft, an der die OSRAM Konzernobergesellschaft oder ein verbundenes Unternehmen eine Minderheitsbeteiligung hält und die sich mit Zustimmung der OSRAM Konzernobergesellschaft auf freiwilliger Basis durch die Unterzeichnung eines ICA auf die Regelungen der BCR verpflichtet hat;
- **BCR** die vorliegenden Binding Corporate Rules und die darin enthaltenen Regelungen;

- **Einwilligung** eine ohne Zwang, spezifische, informierte und unzweideutige Willensäußerung, bei der die betroffene Person durch eine Erklärung oder eine klare positive Handlung ihr Einverständnis mit der Verarbeitung sie betreffender personenbezogener Daten bekundet[2];

- **Verantwortlicher** die Stelle (natürliche oder juristische Person, Behörde oder sonstige rechtlich selbständige Stelle), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet;

- **CDPD** Corporate Data Privacy Department, die gemäß OSRAM Organisationsplan für den konzernweiten Datenschutz zuständige zentrale Abteilung des OSRAM Konzerns;

- **Kunden und Lieferanten** die natürlichen und juristischen Personen, mit denen eine Geschäftsbeziehung besteht oder geplant ist;

- **Betroffener / Betroffene Person** jede bestimmte oder bestimmbare natürliche Person, deren Daten verarbeitet werden. Bestimmbar ist eine Person dann, wenn sie direkt oder indirekt identifiziert werden kann, z. B. durch Bezugnahme auf einen spezifischen Identifikator oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind; Juristische Personen können durch entsprechende Vereinbarung zwischen der datenübermittelnden Gesellschaft und dem Datenempfänger in den Geltungsbereich der BCR einbezogen werden und gelten insoweit als Betroffene;

- **DPC** den Data Protection Coordinator, d.h. Datenschutzkoordinator die von einem teilnehmenden Unternehmen benannte Person, die für die lokale Umsetzung und Einhaltung der BCR sowie für die Unterstützung der CDPD verantwortlich ist;

- **DPE** den Data Protection Executive einer Konzerngesellschaft; diese Position wird vom jeweiligen CEO der Konzerngesellschaft wahrgenommen;

- **DPO** Data Protection Officer, d.h. die von einem teilnehmenden Unternehmen ernannte Person, die die Geschäftsleitung in Fragen der lokalen Umsetzung und Einhaltung der Allgemeinen Datenschutzverordnung und anderer anwendbarer Datenschutzbestimmungen beaufsichtigt und berät und deren Ernennung unter bestimmten, darin festgelegten Bedingungen obligatorisch ist;

- **EWR-Land / EWR-Länder** die Mitgliedsstaaten der Europäischen Union (EU) sowie die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR);

- **Datenschutz-Grundverordnung (DSGVO)** die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

- **Konzerngesellschaft bzw. OSRAM-Konzerngesellschaft** die OSRAM Konzernobergesellschaft und jede in- oder ausländische Gesellschaft, an denen die OSRAM Konzernobergesellschaft direkt oder indirekt mit Mehrheit beteiligt ist bzw. die Mehrheit der Stimmrechte oder die Managementkontrolle besitzt;

- **ICA** Inter-Company Agreement, durch dessen Beitritt sich ein Unternehmen des OSRAM-Konzerns zur Einhaltung der Bestimmungen der BCR verpflichtet;

- **OSRAM Konzernobergesellschaft** die OSRAM GmbH;

- **Teilnehmende Gesellschaft** eine OSRAM-Konzerngesellschaft oder eine beitretende Gesellschaft, die dem ICA beitritt und sich damit zur Einhaltung der Bestimmungen dieser BCR verpflichtet;

- **Personenbezogene Daten** alle Informationen über einen Betroffenen;

- **Verletzung personenbezogener Daten** eine Sicherheitsverletzung, die zur unbeabsichtigten oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum

[2] Bestimmte nationale Gesetzgebungen können besondere Anforderungen an die Einwilligung stellen, was die Gültigkeit der Einwilligung beeinträchtigen kann.

unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt;

- **Verarbeitung personenbezogener Daten** oder **Datenverarbeitung** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten - wie etwa das Erheben, Speichern, die Organisation, Strukturierung, Aufbewahrung, die Anpassung oder Veränderung, das Abfragen, die Konsultation, Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder sonstige Bereitstellung, die Angleichung oder Kombination sowie die Löschung, die Vernichtung oder die Einschränkung der Verarbeitung;

- **Auftragsverarbeiter** die natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet;

- Besondere **Kategorien personenbezogener Daten** Informationen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen; genetische Daten und biometrische Daten, die zur eindeutigen Identifizierung einer natürlichen Person verwendet werden, Daten über die Gesundheit oder Daten über das Sexualleben oder die sexuelle Ausrichtung eines natürlichen Individuums;

- **Standard-Vertragsklauseln** EU-Standardvertragsklauseln für Datenverarbeiter, die durch den Beschluss der Europäischen Kommission 2010/87/EU angenommen wurden, oder EU-Standardvertragsklauseln zwischen Datenverarbeitern, die durch den Beschluss 2011/497/EG oder 2004/915/EG angenommen wurden, oder andere vertragliche Garantien, die durch Beschlüsse der Europäischen Kommission gemäß Artikel 46 Absatz 2 (c) der Datenschutz-Grundverordnung angenommen wurden

- **Dritter** jede natürliche oder juristische Person, Behörde, Einrichtung oder Stelle außer der betroffenen Person, des Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der direkten Aufsicht des Verantwortlichen oder des Auftragsverarbeiters befugt sind, personenbezogene Daten zu verarbeiten

Zusammenfassung der OSRAM BCR

Primäres Ziel dieser Binding Corporate Rules („BCR“) ist es, ein weltweit angemessenes und einheitliches Datenschutzniveau innerhalb des gesamten OSRAM Konzerns bzw. bei allen beitretende Gesellschaften herzustellen und damit den adäquaten Schutz von personenbezogenen Daten, die im Geschäftsablauf von einer teilnehmenden Gesellschaft an andere teilnehmende Gesellschaften übermittelt werden, weltweit sicherzustellen. Unter den Anwendungsbereich dieser BCR fallen dabei folgende personenbezogene Daten:

- Personenbezogene Daten aus der EU / dem EWR, auf die die Datenschutz-Grundverordnung Anwendung findet;
- Personenbezogene Daten ungeachtet ihres Herkunftslandes, sofern sie von einer (datenerhebenden) teilnehmenden Gesellschaft an eine andere (empfangende) teilnehmende Gesellschaft übermittelt wurden.

Hierfür ist es erforderlich, für die Verarbeitung personenbezogener Daten einheitliche Datenschutz- und Datensicherheitsstandards im Sinne der Datenschutz-Grundverordnung festzulegen und so sicherzustellen, dass im Hinblick auf die unter den Schutzbereich dieser BCR fallenden personenbezogenen Daten weltweit ein angemessenes Datenschutzniveau und entsprechende Garantien im Sinne der Datenschutz-Grundverordnung hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gewährleistet werden.

Diese BCR stellen das generelle und allgemeingültige Rahmenregelwerk für die Verarbeitung der unter den Anwendungsbereich der BCR fallenden personenbezogenen Daten von Mitarbeitern, Kunden, Lieferanten, Geschäftspartnern oder künftigen Geschäftspartnern sowie sonstiger Betroffener durch OSRAM-Konzerngesellschaften oder beitretende Gesellschaften dar.
Die vorliegenden BCR berücksichtigen den derzeitigen Stand und die aktuellen Vorgaben im internationalen Datenschutz, insbesondere die Anforderungen der Datenschutz-Grundverordnung, die einschlägigen Richtlinien, die Arbeitsdokumente der Artikel-29-Datenschutzgruppe und des Europäischen Datenschutzausschuss sowie der Grundsätze der Internationalen Konferenz der Datenschutzbeauftragten über Internationale Standards zum Schutz der Privatsphäre (im folgenden: "Madrid -Resolution") vom 5. November 2009.

1. Inhalt der Richtlinie

1.1 Anwendungsbereich der BCR

Alle OSRAM-Konzerngesellschaften und beitretende Gesellschaften weltweit fallen in den Anwendungsbereich dieser bindenden Unternehmensrichtlinie. Die BCR gelten für die Verarbeitung

- aller personenbezogenen Daten aus der EU / dem EWR, auf die die Datenschutz-Grundverordnung Anwendung findet;
- personenbezogener Daten ungeachtet ihres Herkunftslandes, sofern sie von einer (datenerhebenden) teilnehmenden Gesellschaft an eine andere (empfangende) teilnehmende Gesellschaft übermittelt wurden.

Erfasst werden personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten, Aktionären sowie von allen sonstigen – gegenwärtigen oder möglichen - Vertrags- und Geschäftspartnern der teilnehmenden Gesellschaften und sonstiger Betroffener.

Unter den Schutzbereich der BCR fallen dementsprechend nicht nur personenbezogene Daten aus teilnehmenden Gesellschaften mit Sitz in einem EWR-Land, sondern darüber hinaus weltweit **alle** von einer teilnehmenden Gesellschaft stammenden personenbezogenen Daten, sobald diese Daten an eine andere teilnehmende Gesellschaft übermittelt wurden (und damit auch personenbezogene Daten, die von einer teilnehmenden Gesellschaft mit Sitz außerhalb des EWR herrühren und dann an eine andere teilnehmende Gesellschaft übermittelt werden).

1.2 Grundsätze der Verarbeitung personenbezogener Daten und Elemente des Datenschutzrahmens

Bei der Verarbeitung personenbezogener Daten durch teilnehmende Gesellschaften im Rahmen dieser BCR sollten die folgenden Grundsätze und Elemente des Datenschutzrahmens, die sich insbesondere aus der Datenschutz-Grundverordnung und der Madrid-Resolution vom 5. November 2009 ableiten, berücksichtigt werden:

1.2.1 Rechtmäßigkeit und Fairness der Datenverarbeitung

Die Verarbeitung der personenbezogenen Daten hat gesetzeskonform unter Einhaltung der jeweils geltenden gesetzlichen Bestimmungen sowie unter Beachtung der in diesen BCR niedergelegten Prinzipien zu erfolgen.

Sie ist nur zulässig, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Betroffene hat in die Verarbeitung ihrer persönlichen Daten für einen oder mehrere spezifische Zwecke eine Einwilligung erteilt; oder
- Die Datenverarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder um auf Antrag der betroffenen Person vor dem Abschluss eines Vertrags Schritte zu unternehmen; oder
- Die Verarbeitung ist für die Einhaltung einer rechtlichen Verpflichtung erforderlich, der dem Verantwortlichen unterliegt; oder
- Die Verarbeitung ist notwendig, um die lebenswichtigen Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen; oder

Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse

- oder in Ausübung der dem Verantwortlichen übertragenen öffentlichen Gewalt ausgeführt wird; oder
- Die Verarbeitung ist zur Wahrung der berechtigten Interessen erforderlich, die der Verantwortliche oder ein Dritter verfolgt, es sei denn, diese Interessen werden durch die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überlagert;
- Die Verarbeitung ist durch die nationalen Gesetze und Vorschriften, die für die teilnehmende Firma gelten, die die Daten ursprünglich übertragen hat, vorgeschrieben oder erlaubt.

Der Verantwortliche muss es dem Betroffenen ermöglichen, auf einfache, schnelle und effiziente Weise jederzeit seine Einwilligung widerrufen zu können.
Alle teilnehmenden Unternehmen sind verpflichtet, personenbezogene Daten fair zu verarbeiten. Die Datenverarbeitung hat so zu erfolgen, dass sie für die betroffenen Personen zumutbar ist und keine ungerechtfertigten nachteiligen Auswirkungen auf sie hat.

1.2.2 Zweckbestimmung

Personenbezogene Daten dürfen ausschließlich für spezifische, eindeutig festgelegte und rechtmäßige Zwecke verarbeitet werden. In keinem Fall dürfen personenbezogene Daten auf eine Weise verarbeitet werden, die mit den legitimen Zwecken, für die die personenbezogenen Daten erhoben wurden, nicht vereinbar wären. Teilnehmende Gesellschaften sind verpflichtet, die Zweckbestimmung der von einer anderen teilnehmenden Gesellschaft an sie übermittelten Daten bei der Speicherung und weiteren Verarbeitung und Nutzung dieser Daten zu beachten; Zweckänderungen sind nur mit Einwilligung des Betroffenen zulässig oder soweit das jeweilige nationale Recht der übermittelnden teilnehmenden Gesellschaft dies zulässt.

1.2.3 Transparenz

Jede teilnehmende Gesellschaft hat personenbezogene Daten auf transparente Art und Weise zu verarbeiten. Gemäß Artikel 13 und 14 der Datenschutz-Grundverordnung müssen Betroffene, deren personenbezogene Daten von einer teilnehmenden Gesellschaft verarbeitet werden, von der teilnehmenden Gesellschaft (ggf. in Absprache mit der übermittelnden Gesellschaft) über folgendes informiert werden:

- Identität und Kontaktdaten des Verantwortlichen und der übermittelnden Gesellschaft;
- Gegebenenfalls Kontaktdaten des Datenschutzbeauftragten des jeweils teilnehmenden Unternehmens;
- Betroffene Kategorien von personenbezogenen Daten;
- Empfängern oder Kategorien von Empfängern personenbezogenen Daten;
- Zweck der Verarbeitung sowie die rechtliche Grundlage für die Verarbeitung;
- Gegebenenfalls legitime Interessen, die von dem Verantwortlichen oder von einem Dritten verfolgt werden;
- Gegebenenfalls Verweis auf die geeigneten Garantien zum Schutz personenbezogener Daten, die an Empfänger mit Sitz in Drittländern oder internationalen Organisationen übermittelt werden, sowie auf die Mittel, mit denen eine Kopie dieser Garantien erhältlich ist oder wo sie zur Verfügung gestellt wurden;
- Der Zeitraum, für den die persönlichen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien, die zur Bestimmung dieses Zeitraums verwendet werden;
- Das Bestehen des Rechts, von dem Verantwortlichen Zugang zu personenbezogenen Daten und deren Berichtigung oder Löschung oder die Einschränkung der Verarbeitung in Bezug auf den Betroffenen zu beantragen oder der Verarbeitung zu widersprechen, sowie das Recht auf Datenübertragbarkeit;
- Wenn die Verarbeitung auf der Einwilligung eines Betroffenen beruht, das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der auf der Einwilligung beruhenden Verarbeitung vor deren Widerruf beeinträchtigt wird;
- Das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen;
- Ob die Bereitstellung personenbezogener Daten eine gesetzliche oder vertragliche Verpflichtung oder ein Erfordernis für den Abschluss eines Vertrages ist, sowie ob der Betroffene verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Folgen es haben kann, wenn diese Daten nicht bereitgestellt werden;
- Das Vorhandensein automatisierter Entscheidungsfindung, einschließlich der Erstellung von Profilen und, zumindest in diesen Fällen, aussagekräftiger Informationen über die damit verbundene Logik sowie die Bedeutung und die vorgesehenen Folgen einer solchen Verarbeitung für die betroffene Person;
- Die Quelle, aus der personenbezogene Daten stammen, einschließlich öffentlich zugänglicher Quellen (es sei denn, es handelt sich um personenbezogene Daten, die direkt von der betroffenen Person erhoben wurden).

Diese BCR werden allen Betroffenen, die in den Genuss der in Unterabschnitt 1.2.18.1.3 dieses Abschnitts festgelegten Rechte als Drittbegünstigte kommen, zusammen mit den in diesem Unterabschnitt aufgeführten Informationen zur Verfügung gestellt.

Soweit die personenbezogenen Daten nicht direkt beim Betroffenen erhoben wurden, kann die Information ausnahmsweise unterbleiben, wenn der Betroffene bereits informiert ist oder damit ein unverhältnismäßiger Aufwand verbunden wäre.

1.2.4 Datenqualität sowie Datensparsamkeit und Speicherbegrenzung

Personenbezogene Daten müssen sachlich richtig sein und – wenn nötig – auf den neuesten Stand gebracht werden. Es sind angemessene Maßnahmen dafür zu treffen, dass nicht zutreffende oder unvollständige Daten berichtigt oder gelöscht werden.

Die Datenverarbeitung hat sich am Ziel der Datensparsamkeit auszurichten. Es sollen nur die erforderlichen personenbezogenen Daten - d. h. so wenig personenbezogene Daten wie möglich - erhoben, verarbeitet oder genutzt werden. Insbesondere ist von den Möglichkeiten der Anonymisierung Gebrauch zu machen, soweit der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter Daten erfolgen, sind nicht datenschutzrelevant, soweit die Daten den Rückschluss auf den Betroffenen nicht mehr ermöglichen.

Personenbezogene Daten, die für die Geschäftszwecke, für die sie ursprünglich erhoben und gespeichert wurden, nicht mehr benötigt werden, sind zu löschen. Sofern gesetzliche Aufbewahrungsfristen gelten, ist die Verarbeitung der jeweiligen Daten eingeschränkt.

1.2.5 Weiterübermittlung von Daten

Die Weiterübermittlung von personenbezogenen Daten von einer teilnehmenden Gesellschaft an eine nicht teilnehmende Gesellschaft ist nur unter den folgenden Voraussetzungen zulässig:

- Sofern es sich bei der empfangenden Stelle um einen Auftragsverarbeiter handelt, sind die in Artikel 28 der Datenschutz-Grundverordnung festgelegten Bedingungen erfüllt;
- Sofern es sich bei der empfangenden Stelle um einen Verantwortlicher handelt, der zusammen mit einem beteiligten Unternehmen die Zwecke und Mittel der Verarbeitung gemeinsam festlegt, sind die in Artikel 26 der Datenschutz-Grundverordnung festgelegten Anforderungen erfüllt.

Die Weiterübermittlung personenbezogener Daten, die eine teilnehmende Gesellschaft mit Sitz in einem Nicht-EWR-Land (= Datenimporteur) von einer anderen teilnehmenden Gesellschaft mit Sitz in einem EWR-Land (= Datenexporteur) erhalten hat, durch den Datenimporteur an einen Verantwortlichen, externen Empfänger außerhalb der OSRAM Gruppe mit Sitz in einem Nicht-EWR-Land ohne angemessenes bzw. anerkanntes Datenschutzniveau ist nur unter der Voraussetzungen zulässig, dass (i) die empfangende Stelle mit einem angemessenen Schutzniveau für personenbezogene Daten im Sinne der Artikel 45-48 der Datenschutz-Grundverordnung ausgestattet ist, z.B. durch den Abschluss von Standardvertragsklauseln oder (ii) durch die Anwendung von Ausnahmeregelungen für besondere Situationen gemäß Artikel 49 der Datenschutz-Grundverordnung.

1.2.6 Besondere Arten personenbezogener Daten und Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten

- Besondere Kategorien von Personendaten dürfen grundsätzlich nicht verarbeitet werden. Sollte die Verarbeitung besonderer Arten personenbezogener Daten erforderlich sein, muss der Betroffene hierin ausdrücklich einwilligen, es sei denn, die Verarbeitung ist zur Erfüllung der Pflichten und zur Ausübung spezifischer Rechte des Verantwortlichen oder der Betroffenen auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit und des Sozialschutzes erforderlich, soweit sie durch geltendes örtliches Recht oder durch einen Tarifvertrag nach geltendem örtlichen Recht, der angemessene Garantien für die Grundrechte und die Interessen des Betroffenen vorsieht, zulässig ist; oder
- der Betroffene ist physisch oder rechtlich nicht in der Lage, seine Einwilligung zu geben (z. B. bei einem medizinischen Notfall) und die Verarbeitung ist erforderlich, um die vitalen Interessen des Betroffenen oder einer anderen natürlichen Person zu wahren; oder
- der Betroffene die fraglichen Daten bereits offenkundig öffentlich gemacht hat; oder
- Die Verarbeitung ist für die Zwecke der Präventiv- oder Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, der medizinischen Diagnose, der Bereitstellung von Gesundheits- oder Sozialfürsorge oder -behandlung oder der Verwaltung von Gesundheits- oder Sozialfürsorgesystemen und -diensten auf der Grundlage des anwendbaren örtlichen Rechts oder aufgrund eines Vertrags mit einem Angehörigen der Gesundheitsberufe erforderlich und unterliegt der Verpflichtung zur Wahrung des Berufsgeheimnisses.

Vor der Verarbeitung besonderer Arten personenbezogener Daten ist der zuständige DPO bzw. DPC der teilnehmenden Gesellschaft oder die CDPC zu konsultieren

Die Verarbeitung personenbezogener Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten wird in der Regel nicht durchgeführt. Sollte eine Verarbeitung dieser Daten erforderlich sein, so ist sie nur nach vorheriger Rücksprache mit der CDPD unter der Kontrolle der zuständigen Aufsichtsbehörde oder vorbehaltlich angemessener Garantien, wie sie durch die Datenschutz-Grundverordnung und andere anwendbare Datenschutzbestimmungen festgelegt sind, zulässig.

1.2.7 Automatisierte Entscheidungen im Einzelfall

Werden personenbezogene Daten mit dem Ziel verarbeitet, eine automatisierte Einzelentscheidung zu treffen, müssen die berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet werden. Entscheidungen, die für den Betroffenen negative rechtliche Folgen nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten, die der Bewertung einzelner Persönlichkeitsmerkmale dient, gestützt, d.h. nicht ausschließlich durch Verwendung von Informationstechnik getroffen werden. Automatisierte Verfahren dürfen grundsätzlich nur als Hilfsmittel für eine solche Entscheidung genutzt werden.

Eine Ausnahme gilt nur, wenn

- Die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages getroffen wird und die berechtigten Interessen des Betroffenen durch Information über die Logik der Entscheidung und die Möglichkeit zur Stellungnahme gewahrt werden, wobei für den Fall einer Stellungnahme des Betroffenen der Verantwortliche verpflichtet ist, ihre Entscheidung zu überprüfen; oder
- Sofern diese durch ein geltendes lokales Gesetz zugelassen ist; oder
- Sofern die Entscheidung auf der ausdrücklichen Zustimmung der betroffenen Person beruht.

1.2.8 Verzeichnis von Verarbeitungstätigkeiten

Alle teilnehmenden Gesellschaften müssen Aufzeichnungen über die in der jeweiligen Gesellschaft durchgeführten Bearbeitungsaktivitäten dokumentieren und aufbewahren. Jeder DPC oder DPO ist dafür verantwortlich, sicherzustellen, dass Aufzeichnungen über die Verarbeitungsaktivitäten dokumentiert und regelmäßig überprüft werden. Die CDPD bietet den teilnehmenden Gesellschaften Zugang zu einem elektronischen Aufzeichnungen führenden System, in dem Aufzeichnungen festgelegt werden sollten. Die CDPD stellt den teilnehmenden Gesellschaften auch Vorlagen und Anweisungen für die Führung der Aufzeichnungen zur Verfügung und überwacht die Einhaltung dieser Verpflichtung.

1.2.9 Datenschutz-Folgenabschätzung

Wenn eine Verarbeitungstätigkeit in Anbetracht der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung wahrscheinlich zu einem hohen Risiko für die Rechte und die Freiheit der betroffenen Personen führen wird, sind die teilnehmenden Gesellschaften verpflichtet, Datenschutzfolgenabschätzungen gemäß Artikel 35 der Datenschutz-Grundverordnung und den diesbezüglichen Leitlinien der Aufsichtsbehörden durchzuführen. Die CDPD gibt den DPCs und DPOs Leitlinien und Methoden zur Durchführung solcher Datenschutzfolgenabschätzungen an die Hand.

Die rechtlichen Anforderungen an den Inhalt solcher Bewertungen sind zu beachten.

Ergibt eine Datenschutzfolgenabschätzung, dass die Verarbeitung zu einem hohen Risiko führen würde, wenn der Verantwortliche keine Maßnahmen zur Risikominderung ergreift, darf der Verantwortliche die Verarbeitung nicht beginnen oder fortsetzen und muss die zuständige Aufsichtsbehörde gemäß Artikel 36 der Datenschutz-Grundverordnung konsultieren.

1.2.10 Datensicherheit

Unter Berücksichtigung des Standes der Technik, der Kosten der Umsetzung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen haben die teilnehmenden Gesellschaften geeignete technische und organisatorische Maßnahmen zu ergreifen, um die erforderliche Datensicherheit zu gewährleisten, die personenbezogene Daten vor versehentlicher oder unrechtmäßiger Löschung, unbefugter Verwendung, Änderung, vor Verlust, Zerstörung sowie vor unbefugter Weitergabe oder unbefugtem Zugriff schützt. Besondere Kategorien personenbezogener Daten sind besonders zu schützen

Die Sicherheitsmaßnahmen sollen ein der Art der verarbeiteten Daten sowie den mit ihrer Verarbeitung verbundenen Risiken angemessenes Sicherheitsniveau herstellen und sich dabei am Stand der Technik in der Datensicherheit orientieren. Die vorzusehenden Sicherheitsmaßnahmen beziehen sich insbesondere auf Rechner (Server und Arbeitsplatzrechner), Netze bzw. Kommunikationsverbindungen sowie Applikationen.
Zur Sicherstellung eines angemessenen Niveaus technischer und organisatorischer Maßnahmen für den Datenschutz sind die Regeln zur Informationssicherheit (OSRAM Richtlinie IT3000) konzernweit verbindlich eingeführt. Das aktuell gültige Regelwerk zur Informationssicherheit ist im Intranet abrufbar.

Zu den spezifischen Maßnahmen, die zur Gewährleistung eines angemessenen Schutzes personenbezogener Daten eingesetzt werden, gehören Pseudonymisierung und Verschlüsselung persönlicher Daten, Zugangskontrollen, Systemzugangskontrollen, Datenzugangskontrollen, Übertragungskontrollen, Eingabekontrollen, Transportkontrollen, Lagerkontrollen, Jobkontrollen, Verfügbarkeits- und Wiederherstellungskontrollen sowie Segregationskontrollen, um Folgendes zu gewährleisten:

- die fortwährende Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste;
- die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen;
- das Vorhandensein eines Verfahrens zur regelmäßigen Prüfung, Beurteilung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Alle Arbeitsplatzrechner – inklusive mobiler Geräte (z.B. Laptops) - sind passwortgeschützt. Das OSRAM-Intranet verfügt über ein Firewallsystem zum Schutz vor unberechtigtem externem Zugriff auf unternehmensinterne Inhalte. Die Übermittlung personenbezogener Daten innerhalb des unternehmenseigenen Netzwerks erfolgt – soweit aufgrund der Natur und des Verwendungszwecks der personenbezogenen Daten erforderlich – in der Regel verschlüsselt.

1.2.11 Vertraulichkeit der Datenverarbeitung
Personenbezogene Daten dürfen nur von Mitarbeitern der teilnehmenden Gesellschaften erhoben, verarbeitet oder genutzt werden, die dazu autorisiert und unter Einhaltung der Datenschutzbestimmungen besonders hingewiesen sind. Die Zugriffsberechtigung des jeweiligen Mitarbeiters ist dabei nach Art und Umfang seines spezifischen Tätigkeitsfeldes zu begrenzen. Es ist dem Mitarbeiter untersagt, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen. Unbefugt in diesem Sinne sind z. B. auch andere Mitarbeiter, sofern und soweit diese die personenbezogenen Daten nicht zur Erledigung der ihnen obliegenden Fachaufgaben benötigen. Die Vertraulichkeitsverpflichtung besteht über das Ende des Beschäftigungsverhältnisses des betroffenen Mitarbeiters hinaus fort.

1.2.12 Meldung von Verletzungen des Schutzes personenbezogener Daten
Alle teilnehmenden Gesellschaften verpflichten sich, die CDPD unverzüglich über jede (vermutete) Datenverletzung, die personenbezogene Daten im Geltungsbereich dieser BCR betrifft, zu informieren.

Die CDPD bewertet die Art der Datenverletzung und die Kategorien der betroffenen Daten/Datensubjekte sowie deren Folgen für die Rechte und Freiheiten der betroffenen Datensubjekte und stellt fest, ob die fragliche Datenverletzung wahrscheinlich zu einer (hohen) Gefährdung der Rechte und Freiheiten natürlicher Personen führen wird.

Falls erforderlich, koordiniert die CDPD zusammen mit dem jeweiligen DPC/DPO die Meldung der Datenverletzung an die Aufsichtsbehörde oder/und die betroffenen Personen sowie die angemessene Dokumentation aller Datenverletzungen und stellt diese der jeweiligen Behörde auf Anfrage zur Verfügung.

1.2.13 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
Unter Berücksichtigung des Stands der Technik, der Kosten der Durchführung und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der Risiken unterschiedlicher Wahrscheinlichkeit und Schwere der durch die Verarbeitung entstehenden Rechte und Freiheiten natürlicher Personen trifft jede teilnehmende Gesellschaft geeignete technische und organisatorische Maßnahmen, um die Grundsätze des Datenschutzes von vornherein und standardmäßig zu erfüllen.

Zu diesem Zweck verabschieden die teilnehmenden Gesellschaften interne Politiken und führen Maßnahmen durch, die unter anderem darauf abzielen, die Verarbeitung personenbezogener Daten auf ein Mindestmaß zu beschränken, personenbezogene Daten so bald wie möglich zu pseudonymisieren, die Funktionen und die Verarbeitung personenbezogener Daten transparent zu machen, die betroffene Person in die Lage zu versetzen, die Datenverarbeitung zu überwachen, und den Verantwortlichen in die Lage zu versetzen, Sicherheitsmerkmale zu schaffen und zu verbessern.
Die Prozesse und Verfahren sind so zu konzipieren, zu entwickeln und umzusetzen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, die für jeden spezifischen Zweck der Verarbeitung erforderlich sind. Diese Verpflichtung bezieht sich auf (i) die Menge der erhobenen personenbezogenen Daten, (ii) den Umfang ihrer Verarbeitung, (iii) den Zeitraum ihrer Speicherung und (iv) ihre Zugänglichkeit.

1.2.14 Datenverarbeitung im Auftrag

Wenn teilnehmende Gesellschaften eine andere Gesellschaft mit der Verarbeitung personenbezogener Daten im Rahmen dieser BCR beauftragen, sind folgende Maßgaben zu beachten:

- Der Auftragsverarbeiter ist vom Verantwortlichen sorgfältig auszuwählen; es ist ein Auftragsverarbeiter auszuwählen, der die für die datenschutzgerechte Verarbeitung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gewährleisten kann;
- Der Verantwortliche hat dafür Sorge zu tragen und sich regelmäßig davon zu überzeugen, dass der Auftragsverarbeiter die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen vollumfänglich einhält;
- Die Durchführung der Datenverarbeitung im Auftrag muss in einem schriftlich oder anderweitig dokumentierten Vertrag geregelt werden, in dem die Rechte und Pflichten des Auftragsverarbeiters eindeutig festgelegt werden;
- Der Auftragsverarbeiter ist vertraglich zu verpflichten, die vom Auftraggeber erhaltenen Daten nur im Rahmen des Auftrages und der vom Auftraggeber erteilten Weisungen zu verarbeiten. Verarbeitungen zu eigenen Zwecken oder zu Zwecken Dritter müssen vertraglich ausgeschlossen werden, es sei denn, die Verarbeitung ist nach dem anwendbaren örtlichen Recht erforderlich. In diesem Fall hat der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung in dem nach dem anwendbaren örtlichen Recht zulässigen Umfang über diese rechtliche Anforderung zu informieren;
- Der Auftragsverarbeiter muss sicherstellen, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer entsprechenden gesetzlichen Verpflichtung zur Vertraulichkeit unterliegen;
- Der Auftragsverarbeiter darf keinen anderen Auftragsverarbeiter (Unterauftragsverarbeiter) ohne vorherige spezifische oder allgemeine schriftliche Genehmigung des Verantwortlichen beauftragen. Im ersteren Fall hat der Auftragsverarbeiter den Verantwortlichen über beabsichtigte Änderungen bezüglich der Hinzufügung oder des Austauschs anderer Auftragsverarbeiter zu informieren und ihm damit Gelegenheit zu geben, Einwände gegen diese Änderungen zu erheben. Der ursprüngliche Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen voll verantwortlich für die Erfüllung der Verpflichtungen durch den Unterauftragsverarbeiter und für die Einhaltung der Bestimmungen der Datenschutz-Grundverordnung und anderer anwendbarer Datenschutzgesetze;
- Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Auftraggeber durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, bei der Erfüllung der Verpflichtung des Auftraggebers, auf die Anfragen der betroffenen Person zu antworten;
- Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen soll dieser den Verantwortlichen bei der Durchführung geeigneter technischer und organisatorischer Maßnahmen unterstützen, den Verantwortlichen unverzüglich über jede Datenverletzung informieren und die für die Benachrichtigung der Aufsichtsbehörden oder/und der betroffenen Personen über Datenverletzungen erforderlichen Informationen bereitstellen. Der Auftragsverarbeiter sollte den Verantwortlichen auch dabei unterstützen, die Einhaltung der Verpflichtungen gemäß Artikel 32 bis 36 der Datenschutz-Grundverordnung sicherzustellen;
- Der Auftragsverarbeiter soll nach Wahl des Verantwortlichen alle personenbezogenen Daten löschen oder nach Beendigung der Erbringung von Dienstleistungen im Zusammenhang mit der Verarbeitung an den Verantwortlichen zurückgeben und vorhandene Kopien löschen, es sei denn, anwendbare Gesetze schreiben die Speicherung der personenbezogenen Daten vor;
- Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Verpflichtungen nachzuweisen, die in einem zwischen ihnen geschlossenen schriftlichen Vertrag festgelegt und durch die geltenden Datenschutzbestimmungen geregelt sind. Der Auftragsverarbeiter muss auch Audits, die vom Verantwortlichen oder einem anderen von ihm beauftragten Auditor durchgeführt werden, ermöglichen und dazu beitragen;
- Der Verantwortliche bleibt für die Zulässigkeit der Verarbeitung verantwortlich und ist weiterhin Ansprechpartner für die Betroffenen und die Aufsichtsbehörde.

1.2.15 Rechte des Betroffenen

Der Betroffene hat hinsichtlich seiner im Geltungsbereich dieser BCR durch eine teilnehmende Gesellschaft verarbeiteten personenbezogenen Daten die nachfolgend aufgeführten, unabdingbaren Rechte.

- Der Betroffene kann **Auskunft** über die zu ihrer Person gespeicherten personenbezogenen Daten und die Zwecke ihrer Verarbeitung verlangen. Der Betroffene hat auch das Recht auf Auskunft über die Identität des Verantwortlichen, die Kategorien der betroffenen personenbezogenen Daten, die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben wurden oder weitergegeben werden können, und die Quellen, aus denen die Daten stammen, falls sie nicht bei dem Betroffenen erhoben wurden. Das Auskunftsrecht erstreckt sich auch auf den vorgesehenen Zeitraum, für den die personenbezogenen Daten gespeichert werden sollen, sowie auf die logische Struktur der Profilerstellung und der automatisierten Verarbeitungsvorgänge, soweit automatisierte Entscheidungen betroffen sind. Darüber hinaus wird die betroffene Person über die Existenz der Rechte der betroffenen Person gemäß diesem Abschnitt informiert, einschließlich des Rechts, eine Beschwerde bei einer Aufsichtsbehörde einzureichen.
- Die oben genannten Informationen müssen in verständlicher Form bereitgestellt werden; d.h. die betroffene Person hat das Recht, eine Kopie der über sie verarbeiteten personenbezogenen Daten oder zumindest Informationen über diese Daten in knapper, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und deutlicher Sprache zu erhalten. Stellt die Betroffene den Antrag auf elektronischem Wege und wünscht die betroffene Person nichts anderes, so sind die Informationen in einer allgemein üblichen elektronischen Form bereitzustellen. Sind die Anträge der Betroffene offensichtlich unbegründet oder überzogen, insbesondere wegen ihres repetitiven Charakters, so kann der für die Verarbeitung Verantwortliche entweder (i) eine angemessene Gebühr unter Berücksichtigung der Kosten für die Erhebung und Bereitstellung der Informationen erheben oder (ii) es ablehnen, dem Antrag nachzukommen.
- Der Betroffene kann **Berichtigung** seiner personenbezogenen Daten verlangen, wenn sich herausstellt, dass diese unrichtig oder unvollständig sind.
- Der Betroffene hat einen Anspruch auf **Löschung** seiner personenbezogenen Daten, wenn (i) die Datenverarbeitung unzulässig war oder in der Zwischenzeit unzulässig geworden ist, (ii) sobald die Daten für den Verarbeitungszweck nicht mehr erforderlich sind, (iii) wenn die Betroffene die Einwilligung, auf die sich die Verarbeitung stützt, zurückzieht, sofern es keinen anderen Rechtsgrund für die Verarbeitung gibt, (iv) wenn die Betroffenen Einwände gegen die Verarbeitung erheben und es keine zwingenden berechtigten Gründe für die Verarbeitung gibt, oder (v) wenn die Löschungspflicht durch örtliches Recht, dem der Auftraggeber unterliegt, festgelegt ist.
- Berechtigte Löschungsansprüche des Betroffenen sind innerhalb angemessener Frist umzusetzen, sofern und soweit die Verarbeitung ist erforderlich für (i) die Erfüllung einer rechtlichen Verpflichtung, die durch örtliche Gesetze, dem der Verantwortliche unterliegt, festgelegt wurde, oder für (ii) die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen. In Fällen, in denen die gesetzlichen Aufbewahrungsfristen gelten oder die Daten nicht gelöscht werden können, kann die Einschränkung der Verarbeitung der betreffenden Daten auf Antrag der betroffenen Person verwendet werden.
- Der Betroffene hat das Recht, die Verarbeitung personenbezogener Daten **eingeschränkt** zu haben, wenn (i) die Richtigkeit der personenbezogenen Daten bestritten wird, und zwar für einen Zeitraum, der es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen; (ii) die Verarbeitung rechtswidrig ist und der Betroffene sich gegen die Löschung der personenbezogenen Daten wendet und stattdessen die Einschränkung ihrer Verwendung verlangt; (iii) der Verantwortliche die personenbezogenen Daten nicht mehr für die Zwecke der Verarbeitung benötigt, sie aber von der Betroffene für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden, oder (iv) wenn der Betroffene der Verarbeitung und der Überprüfung widersprochen hat, ob die berechtigten Gründe des für die Verarbeitung Verantwortlichen die berechtigten Gründe des Betroffenen überwiegen.
- Der Betroffene hat das Recht, die ihn betreffenden personenbezogenen Daten, die er einem Verantwortlichen zur Verfügung gestellt hat, in einem strukturierten, allgemein üblichen und maschinenlesbaren Format zu **erhalten** und hat das Recht, diese Daten an einen anderen für die Verarbeitung Verantwortlichen zu übermitteln, sofern (i) die Verarbeitung der Daten auf der Einwilligung der Betroffene oder alternativ auf dem Vertrag mit der Betroffene beruht und (ii) die Verarbeitung mit automatisierten Mitteln erfolgt.
- Der Betroffene hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer **automatischen Verarbeitung**, einschließlich der Erstellung von Profilen, beruht und rechtliche Folgen für ihn hat, es sei denn, die Entscheidung ist (i) für den Abschluss oder die Erfüllung eines Vertrags erforderlich, (ii) beruht auf der ausdrücklichen Einwilligung des Betroffenen oder (iii) nach geltendem Recht zulässig.

- Der Betroffene hat das Recht, jederzeit aus Gründen, die mit seiner Situation zusammenhängen, die Verarbeitung seiner personenbezogenen Daten zu **widersprechen**, wenn diese auf dem berechtigten Interesse des Verantwortlichen beruht. Der Verantwortliche darf die betreffenden personenbezogenen Daten nicht mehr verarbeiten, es sei denn, der für die Verarbeitung Verantwortliche weist zwingende legitime Gründe für die Verarbeitung nach, die die Interessen, Rechte und Freiheiten der Betroffene überwiegen, oder für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Der Betroffene hat das Recht, jederzeit gegen die Verarbeitung ihn betreffender personenbezogener Daten für Zwecke des Direktmarketings Einspruch zu erheben, einschließlich der Erstellung von Profilen, soweit diese mit diesem Direktmarketing in Zusammenhang stehen. Widerspricht der Betroffene der Verarbeitung für Zwecke des Direktmarketings, können die personenbezogenen Daten nicht mehr für solche Zwecke verarbeitet werden.
- Der Betroffene hat das Recht, bei einer Aufsichtsbehörde eine Beschwerde einzureichen.
- Der Betroffene hat das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn er der Ansicht ist, dass seine Rechte nach der Datenschutz-Grundverordnung infolge der Verarbeitung ihrer personenbezogenen Daten unter Missachtung der Datenschutz-Grundverordnung verletzt worden sind.
- Beruht die Datenverarbeitung auf der Einwilligung der Betroffene, hat er das Recht, seine Einwilligung jederzeit zu widerrufen.

Der Betroffene kann die vorgenannten Rechte gegenüber der teilnehmenden Gesellschaft, dem zuständigen DPC/DPO der teilnehmenden Gesellschaft oder der CDPD schriftlich geltend machen. Das berechtigte Ersuchen des Betroffenen ist von der kontaktierten Stelle innerhalb einer angemessenen Frist zu beantworten, und zwar grundsätzlich in schriftlicher Form (E-Mail ist ausreichend).

Die teilnehmende Gesellschaft muss die Ausübung der oben aufgeführten Rechte der betroffenen Person erleichtern. Zu diesem Zweck übermittelt die teilnehmende Gesellschaft die Antwort auf die Anfrage der Betroffene ohne unangemessene Verzögerung und auf jeden Fall nicht später als einen Monat nach Eingang der Anfrage.

1.2.16 Verantwortlichkeit

Alle teilnehmenden Gesellschaften sind verpflichtet, Maßnahmen zu ergreifen, um die Einhaltung der Anforderungen der Datenschutz-Grundverordnung und anderer anwendbarer Datenschutzbestimmungen nachzuweisen, insbesondere mit Hilfe der entsprechenden Dokumentation. Zu diesem Zweck müssen sie (i) die Grundsätze und Vorschriften des Datenschutzes und der Informationssicherheit einhalten und umsetzen, (ii) Aufzeichnungen über die Kategorien von Verarbeitungsaktivitäten führen, (iii) die Anforderungen des Datenschutzes von vornherein und standardmäßig einhalten und, falls erforderlich, (iv) schriftliche Verträge mit Datenverarbeitern oder anderen Verantwortlichen abschließen, (v) einen Datenschutzbeauftragten benennen sowie (vi) Datenschutzfolgenabschätzungen durchführen.

Die Verpflichtungen zur Rechenschaftslegung sind fortlaufend, und die getroffenen Maßnahmen sind regelmäßig zu überprüfen und zu aktualisieren.

1.2.17 Beschreibung der Datentransfers

OSRAM verfügt über eine komplexe Konzernstruktur mit einer Vielzahl von teilnehmenden Gesellschaften, zwischen denen personenbezogene Daten für eine Vielzahl von Zwecken ausgetauscht werden. Ein Datenaustausch erfolgt dabei sowohl zwischen teilnehmenden Gesellschaften mit Sitz in einem EWR-Land als auch mit oder zwischen teilnehmenden Gesellschaften mit Sitz außerhalb des EWR.

Betroffen von den konzernweiten Datenaustauschnotwendigkeiten sind personenbezogene Daten von Mitarbeitern, bestehenden und potenziellen Kunden, Lieferanten, Dienstleistern, Aktionären, sonstigen Geschäfts- und Vertragspartnern sowie von Bewerbern und Beschwerdeführern. Dazu können - je nach Verwendungszweck - Mitarbeiter- und Vertragsstammdaten, Beschäftigungsdaten und Beschäftigungshistorie, Daten über Aus- und Weiterbildungsaktivitäten, Mitarbeiterbeurteilungen, Bankkonto- und Kreditkarteninformationen, Kommunikationsinformationen, einige spezielle Kategorien personenbezogener Daten (z.B. Informationen über Ehe, Religionszugehörigkeit, physische und psychische Gesundheit) usw. gehören.

Verarbeitet und übermittelt werden diese Daten im Konzernverbund ausschließlich im Rahmen normaler Geschäftszwecke sowie für Zwecke interner Administration. Die Übermittlung erfolgt somit für Zwecke der Personalgewinnung, Personalverwaltung und Personalentwicklung, für Compliance-Zwecke, zur Abwicklung und Durchführung von Aufträgen und Projekten bei – externen und internen - Kunden, zur Abwicklung von Bestellungen und Beauftragungen bei Lieferanten und Dienstleistern, zur Erfüllung von Berichtspflichten, zur Erfüllung oder zum Einziehen von Verbindlichkeiten, zur Abrechnung, zum Zwecke der internen Kommunikation, zum Zwecke der kostensenkenden Konsolidierung und Bündelung von IT-Prozessen in bestimmten Regionen, sowie im Zusammenhang mit der Kooperation und Koordination von Konzerngesellschaften auf regionaler oder auf globaler Ebene im Zuge globaler Geschäftsvorgänge und Projekte.

1.2.18 Verfahrensfragen

1.2.18.1 Verbindlichkeit der BCR

Die BCR haben einen umfassend verbindlichen Charakter.

1.2.18.1.1 Verbindlichkeit für Konzerngesellschaften und teilnehmende Gesellschaften

Die BCR sind durch die zuständigen Governance Owner des OSRAM Konzerns verabschiedet und durch die Veröffentlichung als Richtlinie CO 3000 (BCR zum Schutz personenbezogener Daten) in Kraft gesetzt worden.

Die Verantwortung für die Umsetzung der BCR in der teilnehmenden Gesellschaft liegt bei der Leitung der teilnehmenden Gesellschaft, die Ausführung im Einzelfall liegt jeweils bei der Stelle innerhalb dieser Gesellschaft, die personenbezogene Daten im Rahmen ihrer Fachaufgabe verarbeitet. Bei OSRAM-Konzerngesellschaften liegt die Verantwortung beim CEO der OSRAM-Konzerngesellschaft in seiner Eigenschaft als Data Protection Executive („DPE“).

Die BCR sind von allen OSRAM Konzerngesellschaften sowie von den beitretenden Gesellschaften verbindlich zu beachten und einzuhalten.

Um den Beitritt und die Umsetzung der BCR zu dokumentieren, tritt im Falle von Konzerngesellschaften die Geschäftsleitung der betreffenden Konzerngesellschaft dem ICA bei. Mit der Unterzeichnung des ICA und der anschließenden Annahme des jeweiligen Antrags durch die OSRAM-Konzernobergesellschaft werden die BCR-Regelungen für das betreffende Konzernunternehmen individuell verbindlich. Der ICA ist von der Leitung der Konzerngesellschaft zu unterzeichnen und an die CDPD bei der OSRAM-Konzernobergesellschaft zurückzusenden. Der ICA ist der BCR als Anlage beigefügt.

Im Grundsatz sind alle OSRAM-Konzerngesellschaften zu einer Unterzeichnung und Umsetzung der BCR verpflichtet, es sei denn, einer OSRAM-Konzerngesellschaft ist wegen des Vorliegens eines triftigen Grundes (z.B. keine Geschäftstätigkeit, keine Mitarbeiter, keine Verarbeitung personenbezogener Daten, anstehende Liquidation oder Veräußerung) ein Dispens von der Umsetzung der BCR erteilt worden. Ein Dispens muss unter Angabe des Grundes hierfür von der OSRAM-Konzerngesellschaft schriftlich oder per email bei der CDPD beantragt werden. Diese entscheidet über die Begründetheit des Antrags und teilt der Konzerngesellschaft die Entscheidung mit. In diesem Fall sind Datentransfers zwischen dieser OSRAM-Konzerngesellschaft und anderen OSRAM-Konzerngesellschaften nur möglich, wenn andere geeignete Schutzmaßnahmen getroffen werden, die ein angemessenes Schutzniveau für personenbezogene Daten gemäß Artikel 45-48 der Datenschutz-Grundverordnung gewährleisten.

Beitretende Gesellschaften, d.h. andere Unternehmen als OSRAM-Konzerngesellschaften, an denen die OSRAM Konzernobergesellschaft direkt oder indirekt beteiligt, können sich auf freiwilliger Basis rechtsverbindlich zur Einhaltung der BCR-Regelungen verpflichten, sofern die CDPD einer solchen Teilnahme zustimmt. Ob anderen Unternehmen als OSRAM-Konzerngesellschaften die Möglichkeit zur freiwilligen Teilnahme am BCR-Verfahren zugebilligt wird, liegt dabei im freien Ermessen der CDPD.

Zur Dokumentation der Anerkennung und Umsetzung der BCR durch eine beitretende Gesellschaft wird zwischen der OSRAM Konzernobergesellschaft und der beitretenden Gesellschaft ein ICA abgeschlossen, dem die BCR als Anlage beigefügt werden. Mit Abschluss des ICA sind die BCR-Regelungen für die beitretende Gesellschaft individuell verbindlich. Der Text des ICA ist diesen BCR als Anlage beigefügt.

Die CDPD führt im OSRAM-Intranet ein elektronisches Verzeichnis der teilnehmenden Gesellschaften, die sich durch ihren Beitritt zum ICA zur Einhaltung der Regelungen der BCR verpflichtet haben, sowie deren Kontaktdaten. Dieses elektronische Verzeichnis (**„Statusübersicht**“) ist im Intranet unter https://privacy.osram.com/DPstatus jederzeit aktuell abrufbar. In der Statusübersicht werden auch diejenigen Konzerngesellschaften geführt und entsprechend kenntlich gemacht, die aufgrund des Vorliegens eines triftigen Grundes von der Unterzeichnung und Umsetzung der BCR ausnahmsweise durch Dispens befreit wurden. Ferner sind die Konzerngesellschaften in der Statusübersicht erfasst und gekennzeichnet, die ihrer Verpflichtung zur Anerkennung und Umsetzung der BCR (noch) nicht nachgekommen sind. Die Statusübersicht ist dem BCR als Anlage beigefügt.

Hat eine Konzerngesellschaft dem ICA (noch) nicht beigetreten, so ist in jedem Einzelfall die Zulässigkeit der Datenübermittlung an diese Konzerngesellschaft zu prüfen und durch geeignete Sondermaßnahmen sicherzustellen, wie beispielsweise durch die Unterzeichnung der EU Standardvertragsklauseln.

Die Verpflichtung zur Einhaltung der BCR kann durch Rücknahme, Widerruf oder Kündigung seitens der OSRAM Konzernobergesellschaft oder seitens der teilnehmenden Gesellschaft beendet werden. Der Verlust des Status einer Konzerngesellschaft führt nicht automatisch zu einer Beendigung der sich aufgrund der BCR ergebenden Verpflichtungen. In diesem Fall ist eine Kündigung der BCR durch die OSRAM Konzernobergesellschaft oder die (ehemalige) Konzerngesellschaft erforderlich. Auch im Falle der Rücknahme bzw. des Widerrufs des ICA oder der Kündigung der BCR bleiben die Verpflichtungen aus der BCR im Hinblick auf die bis zu Rücknahme, Widerruf oder Kündigung verarbeiteten personenbezogenen Daten bestehen, bis diese Daten – im Einklang mit den geltenden gesetzlichen Bestimmungen – durch die betroffene Gesellschaft gelöscht wurden.

1.2.18.1.2 Verbindlichkeit gegenüber Mitarbeitern von teilnehmenden Gesellschaften

Auch die Mitarbeiter der teilnehmenden Gesellschaften sind an die Regelungen der BCR gebunden. Der CEO der jeweiligen teilnehmenden Gesellschaft hat die Verpflichtung, die rechtliche Bindungswirkung der BCR für die Mitarbeiter in geeigneter Weise sicherzustellen.

Die BCR-Regelungen sowie alle sonstigen den Datenschutz betreffenden Regelungen stehen den Mitarbeitern der teilnehmenden Unternehmen jederzeit zur Verfügung.

Die teilnehmenden Gesellschaften unterrichten ihre Mitarbeiter darüber, dass die Nichteinhaltung der BCR-Regelungen zu disziplinarischen oder arbeitsrechtlichen Maßnahmen (z.B. Abmahnung, Kündigung) gegen die Mitarbeiter führen kann.

1.2.18.1.3 Verbindlichkeit gegenüber Betroffenen

Bestimmte Regelungen der BCR sind – im Wege der Drittbegünstigung - auch gegenüber Betroffenen verbindlich. Drittbegünstigenden Charakter haben die Regelungen in den Ziffern 1.2.1 – 1.2.7, 1.2.10 - 1.2.15, 1.2.18.1.3, 1.2.18.2, 1.2.18.6, 1.2.18.9, 1.2.18.10 und 1.2.19.

Die Betroffenen sind berechtigt, die Einhaltung eines der vorgenannten drittbegünstigenden Rechte durch eine teilnehmende Gesellschaft durch eine Beschwerde bei der zuständigen Aufsichtsbehörde oder durch die Geltendmachung eines sonstigen Rechtsmittels bei den zuständigen Gerichten durchzusetzen. Die Betroffenen können dabei Schadensersatz geltend machen.

Die Betroffenen können ihre Ansprüche nach ihrer Wahl geltend machen

- bei der Aufsichtsbehörde oder am Gerichtsstand der in einem EWR-Land belegenen teilnehmenden Gesellschaft, die die Daten übermittelt hat; oder
- bei der zuständigen Aufsichtsbehörde oder am Gerichtsstand der Mitgliedstaaten, in denen die betroffene Person ihren gewöhnlichen Aufenthalt oder ihren Arbeitsplatz hat, wenn die betroffene Person im EWR-Land wohnt; oder
- bei der Aufsichtsbehörde oder am Gerichtsstand in dem EWR-Land, in dem sich der Hauptsitz der Obergesellschaft des OSRAM-Konzerns befindet; oder
- bei der zuständigen Aufsichtsbehörde.

Im Falle eines Verstoßes gegen die Regelungen der BCR durch eine teilnehmende Gesellschaft mit Sitz außerhalb des EWR sind somit auch Gerichte und Behörden im EWR zuständig. Dem Betroffenen stehen in diesen Fällen gegenüber der OSRAM Konzernobergesellschaft dieselben Rechte zu, als wenn der Verstoß von der OSRAM Konzernobergesellschaft begangen worden wäre und nicht von einer teilnehmenden Gesellschaft mit Sitz außerhalb des EWR.

Um die Drittbegünstigung der Betroffenen auch in den Ländern sicherzustellen, in denen eine Einräumung der Drittbegünstigung im BCR-Dokument womöglich nicht ausreicht, wird OSRAM – soweit erforderlich – entsprechende zusätzliche vertragliche Vereinbarungen mit den betroffenen teilnehmenden Gesellschaften aufsetzen. Eine Drittbegünstigungsklausel, die den Betroffenen die erforderlichen Rechte einräumt, ist in dem ICA enthalten, die die Konzern- und beitretende Gesellschaften als Zeichen ihrer Akzeptanz und Umsetzung der BCR unterschreiben.

1.2.18.2 Publizität der BCR

Die BCR und die Drittbegünstigungsklausel sind für die Betroffenen einfach zugänglich. Der Betroffene kann sich entweder an den zuständigen DPC oder DPO der teilnehmenden Gesellschaft oder aber direkt an die OSRAM Konzernobergesellschaft wenden. Zusammen mit den unter Abschnitt 1.2.3. („Transparenz“) aufgeführten Informationen wird OSRAM den Betroffenen die BCR in geeigneter Weise zugänglich machen, insbesondere durch die Veröffentlichung der jeweils aktuellen Version der BCR auf den OSRAM Internetseiten. Weitere einschlägige BCR Dokumente – namentlich die Anlagen zu den BCR – werden dem Betroffenen auf Anfrage von der CDPD zur Verfügung gestellt.

1.2.18.3 Umsetzung der BCR in den teilnehmenden Gesellschaften

Die Leitung einer teilnehmenden Gesellschaft - bzw. der CEO einer teilnehmenden Konzerngesellschaft in seiner Eigenschaft als DPE - ist verantwortlich für eine ordnungsgemäße Umsetzung und Befolgung der BCR. Die Leitung der teilnehmenden Gesellschaft kann diese Aufgabe – nicht aber die Verantwortung - auf den DPC oder den DPO delegieren.

OSRAM hat ein weltweites Netzwerk von DPCs und DPOs eingerichtet. Beim Beitritt des ICA zu den BCR erkennt jede teilnehmende Gesellschaft einen DPC oder, falls erforderlich, einen DPO und übermittelt dessen Kontaktdaten an die CDPD. Änderungen in der Person des DPC oder DPO sind der CDPD durch die teilnehmende Gesellschaft unverzüglich anzuzeigen.

Der DPC oder der DPO dient (i) als lokale Kontaktstelle für die betroffenen Personen, d. h. im Rahmen des Beschwerdeverfahrens, (ii) überwacht die Umsetzung und Einhaltung der BCR, (iii) konsultiert die Mitarbeiter in Fragen des Datenschutzes, (iv) erleichtert die Zusammenarbeit zwischen der CDPD, der Revisionsabteilung oder den Aufsichtsbehörden und einer teilnehmenden Gesellschaft in Fragen und (v) führt und aktualisiert notwendige Aufzeichnungen über die Verarbeitungstätigkeiten und Datenschutzfolgenabschätzungen im Sinne der Grundsätze der Rechenschaftspflicht.

Der DPO/DPC berichtet einmal jährlich an die Leitung der betreffenden teilnehmenden Gesellschaft und der DPC berichtet - mindestens jährlich - an die CDPD. Dabei berichtet der DPO/DPC insbesondere auch jeweils über den Umsetzungsstand der BCR bei der teilnehmenden Gesellschaft.

Der Leiter der CDPD steht der CDPD vor und koordiniert und führt alle DPCs und DPOs der teilnehmenden Gesellschaften. Der Leiter der CDPD untersteht dem CIO der OSRAM Konzernobergesellschaft, der wiederum dem CFO der OSRAM Konzernobergesellschaft unterstellt ist. Der Leiter der CDPD koordiniert und treibt die konzernweite Umsetzung der BCR bei den teilnehmenden Gesellschaften, insbesondere die Sammlung der ICAs, Beratung und Anleitung der DPC bei der Umsetzung der BCR sowie durch Einholung und Auswertung regelmäßiger Berichte der DPC/DPO zum Datenschutz sowie zur BCR-Implementierung. Auch ist er für die Erstellung geeigneter BCR Trainings sowie für die Verfügbarmachung solcher BCR Trainings an die teilnehmenden Gesellschaften verantwortlich. Der Leiter der CDPD ist ferner für die Aktualisierung der BCR sowie für die Kommunikation solcher Änderungen an die zuständigen Datenschutzaufsichtsbehörden zuständig. Der Leiter wird durch die CDPD bei der Wahrnehmung seiner Aufgaben unterstützt.

Der Leiter der CDPD berichtet einmal jährlich an die Geschäftsleitung der OSRAM Konzernobergesellschaft. Gegenstand dieses Berichts ist insbesondere auch der Umsetzungsstand der BCR bei allen teilnehmenden Gesellschaften.

1.2.18.4 Überwachung der Einhaltung der BCR

Die Einhaltung der BCR durch die teilnehmenden Gesellschaften wird primär regelmäßig durch den von der Leitung der teilnehmenden Gesellschaft benannten DPC oder DPO überprüft. Die Leitung der teilnehmenden Gesellschaft unterstützt den DPC bei der Wahrnehmung seiner Aufgaben und bindet ihn im Falle von Beschwerden von Betroffenen wegen Nichteinhaltung der BCR ein.

Im Falle Datenschutzverstöße sowie bei Problemen von grundlegender Bedeutung konsultiert der jeweilige DPC/DPO den Leiter der CDPD und berücksichtigt dessen Hinweise und Entscheidungen bei der Beseitigung solcher Datenschutzverstöße und Probleme.

Die OSRAM Konzernobergesellschaft ist berechtigt, die Tätigkeit der DPC im Zusammenhang mit der Implementierung und Einhaltung der BCR in der teilnehmenden Gesellschaft stichprobenartig zu prüfen, entweder durch Anfordern eines schriftlichen Self Assessments des DPC/DPO oder im Rahmen von Kontrollinterviews. Der Inhalt solcher Kontrollgespräche ist vom Auditor zu dokumentieren.

Jede datenübermittelnde teilnehmende Gesellschaft hat das Recht, die Datenverarbeitung bei der empfangenden teilnehmenden Gesellschaft im Einzelfall zu überprüfen. Die übermittelnde Gesellschaft wird dabei die festgestellten Rechte der Betroffenen wahrnehmen und Betroffene, die durch die Verletzung der sich aus diesen BCR ergebenden Verpflichtungen einen Schaden erlitten haben, bei der Durchsetzung ihrer Rechte gegen die verantwortliche Gesellschaft unterstützen.

1.2.18.5 Schulung

Ein zentraler Aspekt der ordnungsgemäßen Umsetzung der BCR ist die entsprechende Unterrichtung und Instruktion der Mitarbeiter. Hierzu zählt auch der Hinweis, dass Verstöße gegen die BCR strafrechtliche, haftungsrechtliche oder arbeitsrechtliche Konsequenzen für den Mitarbeiter nach sich ziehen können.

OSRAM bietet individuelle Informationen sowie spezielle Schulungsmaßnahmen zu den BCR an, die auf eine angemessene Information und Schulung der Mitarbeiter einer teilnehmenden Gesellschaft zum korrekten Umgang mit sowie zum Schutz personenbezogener Daten im Rahmen der Umsetzung der BCR abzielen. Adressat der Schulungsmaßnahmen sind insbesondere die Mitarbeiter, die ständigen oder regelmäßigen Umgang mit personenbezogenen Daten haben. Für diese Mitarbeiter ist die Teilnahme an den Schulungen verpflichtend. Die Schulungen zu den BCR sind in regelmäßigen, angemessenen Abständen zu wiederholen.

Informations- und Schulungsmaßnahmen können – unter anderem – die Durchführung von Web Based Trainings („WBT“), das Angebot geeigneter Präsentationen und Schulungsmaterialien zum Selbststudium, Präsenzschulungen sowie die Organisation von speziell auf Mitarbeiter zugeschnittenen Workshops umfassen.

Die erfolgreiche Teilnahme der Mitarbeiter an der Schulung ist zu dokumentieren.

Weitere Einzelheiten sind in einem detaillierten Schulungskonzept geregelt.

1.2.18.6 Internes Beschwerdeverfahren

Jeder Betroffene kann sich jederzeit mit Beschwerden wegen Verstoßes gegen die BCR durch eine teilnehmende Gesellschaft sowie mit Fragen an die zuständige interne Beschwerdestelle (CDPD; Kontaktdaten vgl. Nummer 1.2.20 Kontakt) oder den lokal zuständigen Datenschutzansprechpartner der teilnehmenden Gesellschaft (i.d.R. der DPC/DPO) wenden. Der Eingang der Beschwerde bei der kontaktierten Stelle ist dem Betroffenen zeitnah zu bestätigen und die Beschwerde innerhalb angemessener Frist – in jedem Fall innerhalb eines (1) Monats ab Eingang der Beschwerde - zu beantworten. Mit der Eingangsbestätigung wird der Betroffene zugleich darüber informiert, welche konkrete Stelle – d.h. die zentrale CDPD oder der lokale DPC/DPO – die Beschwerde bearbeiten wird.

Die bei der zuständigen Beschwerdestelle mit der Beschwerdebearbeitung befassten Mitarbeiter verfügen über ein hinreichendes Maß an Unabhängigkeit bei der Wahrnehmung dieser Aufgabe.

Die teilnehmende Gesellschaft und die CDPD sind bei Anfragen verpflichtet, mit den Aufsichtsbehörden im jeweiligen Land zu kooperieren und deren Entscheidung zu respektieren.

Weitere Einzelheiten – Form der Beschwerde, Bearbeitungsfristen, weiteres Vorgehen bei Anerkennung und/oder Ablehnung der Beschwerde, weiterführende Rechtsbehelfe - sind in einem separaten Beschwerdekonzept geregelt.

1.2.18.7 BCR Audit

OSRAM hat das im Konzern bereits existierende interne Audit- und Kontrollsystem um ein BCR Audit Programm ergänzt, um sicherzustellen, dass die Einhaltung eines angemessenen Datenschutzniveaus nach Maßgabe der BCR-Regelungen in den teilnehmenden Gesellschaften regelmäßig kontrolliert wird.

Die primäre Zuständigkeit für die Durchführung von turnusmäßigen papierbasierten BCR Audits, turnusmäßigen Vor-Ort BCR Audits sowie von anlassbezogenen ad-hoc BCR Audits liegt bei der OSRAM Auditabteilung. Alternativ kann ein BCR Audit im Bedarfsfall auch von einem akkreditierten externen Auditor vorgenommen werden.

Den Zeitplan für die turnusmäßigen BCR Audits legt die OSRAM Auditabteilung im Einklang mit ihrer allgemeinen Audit Zeitplanung fest.

Einmal jährlich findet ein papierbasiertes BCR Audit in Gestalt eines Self Assessments (Ausfüllen eines Fragebogens) durch die teilnehmende Gesellschaft statt. Der Leiter der CDPD und die OSRAM Auditabteilung erhalten die Ergebnisse dieses turnusmäßigen Self Assessments.

Im Falle besonderer Umstände (z.B. Datenschutzvorfälle, Beschwerden Betroffener, bei Self Assessments festgestellte Defizite) können die CDPD oder die Abteilung für Informationssicherheit (IT DIS) neben den vorgenannten geplanten, turnusmäßigen BCR Audits auch noch weitere ad-hoc BCR Audits beauftragen.

Das BCR Audit bezieht sich auf alle Aspekte der BCR. Soweit ein BCR Audit zu dem Ergebnis kommt, dass Abhilfemaßnahmen wegen eines BCR-Verstoßes zu treffen sind, hat das BCR Audit auch für eine Umsetzung der erforderlichen Abhilfemaßnahmen Sorge zu tragen.

Der Leiter der CDPD, die Geschäftsleitung des OSRAM Konzerns und die Leitung der geprüften teilnehmenden Gesellschaft erhalten den vollständigen BCR Auditbericht. Die Ergebnisse des BCR Audits werden der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt. Soweit erforderlich, kann OSRAM hierbei Teile der Prüfungsdaten unkenntlich machen, um den Schutz vertraulicher Unternehmensinformationen sicherzustellen.

Die zuständige Aufsichtsbehörde hat das Recht, ein eigenes BCR Audit bei einer teilnehmenden Gesellschaft durchzuführen. Die Behörde kann das BCR Audit entweder selber oder mittels eines akkreditierten unabhängigen Auditors durchführen. Ein behördliches BCR Audit beschränkt sich ausschließlich auf die Einhaltung der BCR durch die teilnehmende Gesellschaft. Beschränkungen aus Vertraulichkeitsvereinbarungen oder aus Geschäfts- und Betriebsgeheimnissen sind zu beachten.

Einzelheiten des BCR Audits sind in einem separaten BCR-Audit-Konzept geregelt.

1.2.18.8 BCR Aktualisierung & Change Management

OSRAM behält sich das Recht zu einer jederzeitigen Änderung und/oder Aktualisierung dieser BCR vor. Eine solche Aktualisierung der BCR kann insbesondere durch geänderte rechtliche Anforderungen, durch maßgebliche Änderungen in der Konzernstruktur oder durch Auflagen der zuständigen Aufsichtsbehörden geboten sein.

Gravierende Änderungen der BCR bedürfen unter Umständen einer erneuten Genehmigungserteilung durch die zuständigen Aufsichtsbehörden.

Alle übrigen Änderungen der BCR sind auch ohne solche erneute Genehmigung möglich, sofern die CDPD eine vollständig aktualisierte Liste aller teilnehmenden Gesellschaften führt und alle Aktualisierungen der Vorschriften verfolgt und aufzeichnet und den betroffenen Personen oder Aufsichtsbehörden auf Anfrage die erforderlichen Informationen zur Verfügung stellt. Die Liste aller operativen Unternehmen der OSRAM-Gruppe und deren BCR-Annahmestatus ist im OSRAM-Intranet unter https://privacy.osram.com/DPstatus zu finden.

Änderungen der BCR sind ohne erneute Genehmigung möglich, wenn keine Übertragung auf eine neue teilnehmende Gesellschaft erfolgt, bis dieses wirksam an die BCR gebunden ist und die Einhaltung der BCR gewährleisten kann. Alle Änderungen der BCR oder der Liste der teilnehmenden Gesellschaften sollten einmal jährlich der zuständigen Aufsichtsbehörde gemeldet werden. Würde eine Änderung möglicherweise das durch die BCR gebotene Schutzniveau beeinträchtigen oder sich erheblich auf die BCR auswirken, muss sie der zuständigen Aufsichtsbehörde unverzüglich mitgeteilt werden.

Die CDPD führt eine Übersicht über alle seit Inkrafttreten der BCR vorgenommenen Änderungen / Aktualisierungen der BCR. Sie führt ferner eine regelmäßig aktualisierte Liste aller teilnehmenden Gesellschaften, die wirksam an die BCR gebunden sind („Statusübersicht“, vgl. Abschnitt 1.2.18.1.1). Die entsprechenden Informationen sind im OSRAM-Intranet unter https://privacy.osram.com/DPstatus zu finden.

Änderungen der BCR sowie Änderungen der Statusübersicht teilt der CDPD denjenigen Aufsichtsbehörden, die die BCR genehmigt haben auf Anfrage, und nach offizieller Genehmigung der BCR mindestens einmal jährlich mit. Solche Mitteilungen enthalten eine summarische Begründung für die vorgenommenen Änderungen.

1.2.18.9 Kooperation untereinander und mit den Aufsichtsbehörden
Alle teilnehmenden Gesellschaften werden bei Anfragen und Beschwerden Betroffener im Hinblick auf die Nichteinhaltung der BCR vertrauensvoll zusammenarbeiten und einander unterstützen.

Die teilnehmenden Gesellschaften verpflichten sich ferner, im Zusammenhang mit der Implementierung der BCR vertrauensvoll mit den zuständigen Aufsichtsbehörden zusammenzuarbeiten. Sie werden auf BCR-bezogene Anfragen der Aufsichtsbehörde innerhalb angemessener Frist und auf angemessene Weise antworten und die Ratschläge und Entscheidungen der zuständigen Datenschutzaufsichtsbehörde im Hinblick auf die Umsetzung der BCR befolgen.

1.2.18.10 Verhältnis der BCR zu lokalen gesetzlichen Regelungen
Die Zulässigkeit der Verarbeitung personenbezogener Daten beurteilt sich anhand des für die übermittelnde teilnehmende Gesellschaft jeweils anwendbaren lokalen Rechts. Soweit das anwendbare lokale Recht einen stärkeren Schutz personenbezogener Daten vorschreibt als diese BCR, richtet sich die Datenverarbeitung nach dem anwendbaren Recht. Jede teilnehmende Gesellschaft muss selbst prüfen (z. B. durch ihren Datenschutzbeauftragten, DPC/DPO oder durch die Rechtsabteilung), ob es solche lokalen gesetzlichen Regelungen (z.B. Datenschutzgesetze) gibt und deren Einhaltung sicherstellen. Sofern das anwendbare lokale Recht ein niedrigeres Schutzniveau für personenbezogene Daten vorsieht als diese BCR, finden die vorliegenden BCR Anwendung.

Falls sich aus dem anwendbaren lokalen Recht ergebende Verpflichtungen im Widerspruch zu den BCR stehen, hat die teilnehmende Gesellschaft unverzüglich den CDPD zu informieren, es sei denn, es besteht ein anderweitiges Verbot, z. B. im Falle eines strafrechtlichen Verbots zur Wahrung der Vertraulichkeit einer strafrechtlichen Untersuchung. Die CDPD wird den Konflikt in die Statusübersicht (vgl. Abschnitt 1.2.18.1.1) eintragen.

Die CDPD wird alle teilnehmenden Gesellschaften, die zuvor Daten an die betreffende teilnehmende Gesellschaft übermittelt haben, über den gemeldeten Widerspruch der BCR mit dem lokalen Recht informieren. Sie wird ferner die zuständige Aufsichtsbehörde über den Regelkonflikt informieren und gemeinsam mit der Datenschutzaufsicht und der teilnehmenden Gesellschaft nach einer praktikablen Lösung suchen, die den Grundsätzen der Datenschutz-Grundverordnung möglichst nahekommt.

Die zuständige Aufsichtsbehörde ist in jedem Fall zu benachrichtigen, wenn eine rechtliche Anforderung, der eine teilnehmende Gesellschaft unterliegt, wahrscheinlich erhebliche nachteilige Auswirkungen auf die durch die BCR gewährten Garantien haben wird, z.B. im Falle eines rechtsverbindlichen Antrags auf Offenlegung der personenbezogenen Daten durch eine Strafverfolgungsbehörde oder ein Staatssicherheitsorgan.

Wenn die Meldung an die CDPD oder an die zuständige Aufsichtsbehörde ausgesetzt oder strafrechtlich verboten wird, um die Vertraulichkeit einer Strafverfolgungsuntersuchung zu wahren, bemüht sich das beteiligte Unternehmen nach besten Kräften, das Recht auf Aufhebung dieser Aussetzung bzw. dieses Verbots zu erwirken, um so viele Informationen wie möglich und so schnell wie möglich übermitteln und nachweisen zu können, dass es dies getan hat. Wenn die Meldung an die zuständige Aufsichtsbehörde nicht möglich ist, muss das teilnehmende Unternehmen der zuständigen Aufsichtsbehörde jährlich allgemeine Informationen über die bei ihm eingegangenen Anträge vorlegen (z.B. Angabe der Anzahl der Anträge auf Offenlegung, Art der angeforderten Daten, Antragsteller, wenn möglich, usw.).

Die teilnehmende Gesellschaft stellt sicher, dass die Übermittlung personenbezogener Daten an eine öffentliche Behörde nicht massiv, unverhältnismäßig und unterschiedslos in einer Weise erfolgen kann, die über das in einer demokratischen Gesellschaft erforderliche Maß hinausgeht.

1.2.19 Haftung
Jede teilnehmende Gesellschaft haftet für die von ihr begangenen Verstöße gegen die BCR.

Die OSRAM Konzernobergesellschaft übernimmt die Haftung für die Nichteinhaltung der BCR durch teilnehmende Gesellschaften mit Sitz außerhalb des EWR, einschließlich der Verpflichtung zur Zahlung von Schadensersatz im Falle eines nachgewiesenen Verstoßes gegen die BCR sowie einer daraus resultierenden Rechtsverletzung des Betroffenen. Sie wird ferner die erforderlichen Abhilfemaßnahmen ergreifen, um Verstöße gegen die BCR durch eine teilnehmende Gesellschaft mit Sitz außerhalb des EWR zu beseitigen.

Die Beweislast trägt die OSRAM Konzernobergesellschaft. Sie muss nachweisen, dass kein Verstoß gegen die BCR vorliegt oder dass der Verstoß gegen die BCR, mit dem der Betroffene seine Schadensersatzforderung begründet, der teilnehmenden Gesellschaft mit Sitz außerhalb des EWR nicht zuzurechnen ist.

Wenn die OSRAM Konzernobergesellschaft nachweisen kann, dass die teilnehmende Gesellschaft mit Sitz außerhalb des EWR nicht für einen BCR-Verstoß haftbar ist, kann sie auch sich selbst von einer diesbezüglichen Verantwortung freizeichnen.

1.2.20 Kontakt

Betroffene können sich mit ihren Anliegen an den DPC/DPO der betreffenden teilnehmenden Gesellschaft oder an den OSRAM CDPD:

OSRAM GmbH

Corporate Data Privacy Department
Marcel-Breuer-Str. 6
D-80807 Munich
Phone: +49 (89) 6213-3889
Email: privacy@osram.com
Internet: https://www.osram.com